IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please AMEND claims 1, 9-13, 17, and 19-22 in accordance with the following:

1. (currently amended) A code execution apparatus using a multiprocessor system, comprising:

a secure memory storing an encrypted code of a secure task and verifying information for verification of validity of the encrypted code, said encrypted code being generated by assigning a signature in units of a page;

a secure processor executing the encrypted code when the validity of the encrypted code is verified according to the verifying information;

a normal memory storing a code of a normal task;

a normal processor executing the code of the normal task;

a controller discriminating between the secure task and the normal task, and storing the encrypted code in the secure memory and the code of the normal task in the normal memory responsive to the discrimination.

2. (original) The apparatus according to claim 1, wherein

said secure memory stores the encrypted code in units of physical memory allocation, stores the verifying information for the encrypted code in the units, and verifies the encrypted code in the units according to the verifying information, and the secure processor fetches, decrypts, and executes an encrypted instruction included in an encrypted code whose validity has been verified.

3. (original) The apparatus according to claim 1, wherein

said secure processor holds a plurality of decryption keys, and decrypts the encrypted instruction using a specified decryption key in the plurality of decryption keys.

4. (original) The apparatus according to claim 2, wherein

said secure memory and said secure processor share a session key after mutual authentication, said secure memory further encrypts the encrypted instruction using the session key, and transfers the encrypted instruction to the secure processor.

5. (original) The apparatus according to claim 1, further comprising

a secure drive further encrypting the encrypted code using a unique key, and storing the encrypted code, wherein

said secure drive and said secure memory share a session key after mutual authentication, said secure drive decrypts the encrypted code using the unique key at a read instruction from said controller, encrypts the code using the session key, and transfers the code to said secure memory.

6. (original) The apparatus according to claim 1, wherein

at least parts of said secure memory and said normal memory overlap each other.

7. (original) The apparatus according to claim 1, wherein

said secure processor fixes at least a part of a logical circuit for executing an encrypted code in a circuit state in a non-volatile manner using the encrypted code.

8. (original) The apparatus according to claim 7, wherein

said secure processor erases a previous circuit state of the logical circuit, and newly overwrites the state.

9. (currently amended) A memory, comprising:

a device storing an encrypted code in units of physical memory allocation, said encrypted code being generated by assigning a signature in units of a page;

a device storing a plurality of pieces verifying information for verification of validity of respective units of the encrypted code; and

a device verifying the respective units of the encrypted code according to the plurality of pieces of verifying information.

10. (currently amended) A processor, comprising:

a device receiving a notification that the encrypted code is valid, from a memory storing the encrypted code and verifying validity of the encrypted code, said encrypted code being generated by assigning a signature in units of a page;

a device fetching and decrypting an encrypted instruction contained in the encrypted code when the notification is received; and

a device executing a decrypted instruction.

11. (currently amended) A computer-readable storage medium recording a program for a computer, said program enabling the computer to perform:

allocating a secure task and a normal task in a multiprocessor system having a secure processor for performing the secure task and a normal processor for performing the normal task;

discriminating between the secure task and the normal task, storing the encrypted code of the secure task and verifying information for verification of validity of the encrypted code in a secure memory, said encrypted code being generated by assigning a signature in units of a page; and

allowing the secure processor to execute the encrypted code when the validity of the encrypted code is verified according to the verifying information.

12. (currently amended) A computer readable storage storing a program for a computer, said program enabling the computer to perform:

allocating a secure task and a normal task in a multiprocessor system having a secure processor for performing the secure task and a normal processor for performing the normal task;

discriminating between the secure task and the normal task;

storing the normal code in a normal memory;

storing the encrypted code of the secure task and verifying information for verification of validity of the encrypted code in a secure memory, said encrypted code being generated by assigning a signature in units of a page; and

allowing the secure processor to execute the encrypted code when the validity of the encrypted code is verified according to the verifying information.

13. (currently amended) A code distributing method, comprising:

a code generator providing an executable code for a code authentication organization, said code being generated by assigning a signature in units of a page;

said code authentication organization adding to the code verifying information for verification of validity of the code, and distributing the code to a user of a multiprocessor system; and

said multiprocessor system including a secure processor for performing a secure task using the code, and a normal processor for performing a normal task, discriminating between the secure task and the normal task, allocating the secure task and the normal task responsive to the discrimination, verifying the validity of the code according to the verifying information, and executing the code.

14. (original) The method according to claim 13, wherein

said code authentication organization presents a fee to the code generator and collects the code, pays the fee when the code is collected, presenting a code fee to the user, adds the verifying information, provides the code for the user, and simultaneously collects the code fee.

15. (original) The method according to claim 13, wherein

said code authentication organization divides the code into two or more divisions, first distributes a part, and then distributes rest of the code to the user at a request of the user.

16. (original) The method according to claim 15, wherein

said code authentication organization presents a fee to the code generator and collects the code, pays the fee when the code is collected, presents a code fee for the rest of the code to the user, adds verifying information, and provides the code and receives the code fee.

17. (currently amended) A code distributing method, comprising:

a code generator providing an executable code for a code authentication organization, and paying a commission, said code being generated by assigning a signature in units of a page;

said code authentication organization adding to the code verifying information for verification of validity of the code;

said code generator distributing the code to a user of a multiprocessor system, and receiving a fee paid by the user; and

said multiprocessor system containing a secure processor for performing a secure task using the code, and a normal processor for performing a normal task, discriminating the secure task and the normal task, allocating the secure task and the normal task responsive to the

discrimination, verifying the validity of the code according to the verifying information, and executing the code.

18. (original) The method according to claim 17, wherein

said code generator divides the code into two or more divisions, first distributes a part, then presents a fee for rest of the code at a request of the user, provides the code, and receives the fee.

19. (currently amended) A code execution apparatus using a multiprocessor system, comprising:

secure memory means for storing an encrypted code of a secure task and verifying information for verification of validity of the encrypted code, said encrypted code being generated by assigning a signature in units of a page;

secure processor means for executing the encrypted code when the validity of the encrypted code is verified according to the verifying information;

normal memory means for storing a code of a normal task;

normal processor means for executing the code of the normal task;

control means for discriminating the secure task and the normal task, allocating the secure task and the normal task, and storing the encrypted code in said secure memory means and the code of the normal task in said normal memory means responsive to the discrimination.

20. (currently amended) A memory, comprising:

means for storing an encrypted code in units of physical memory allocation, said encrypted code being generated by assigning a signature in units of a page;

means for storing a plurality of pieces of verifying information for verification of validity of respective units of the encrypted code; and

means for verifying the respective units of the encrypted code iaccording to plurality of pieces of the verifying information.

21. (currently amended) A processor, comprising:

means for receiving a notification that an encrypted code is valid, from a memory storing the encrypted code and verifying validity of the encrypted code, said encrypted code being generated by assigning a signature in units of a page;

means for fetching and decrypting an encrypted instruction contained in the encrypted code when the notification is received; and

means for executing a decrypted instruction.

22. (currently amended) A method, comprising:

executing encrypted code of a secure task when validity of the encrypted code is verified according to verifying information, said encrypted code being generated by assigning a signature in units of a page;

executing code of a normal task; and

discriminating between the secure task and the normal task, and storing the encrypted code in a secure memory and the code of the normal task in a normal memory responsive to the discrimination.